NASA Policy Directive

NPD 2810.1D
Effective Date: May 09, 2009
Expiration Date: May 09, 2014

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Information Security Policy

Responsible Office: Office of the Chief Information Officer

1. POLICY

This NASA Policy Directive consolidates information security policy for both classified and unclassified information. Responsibility for information security is shared between the Office of the Chief Information Officer (OCIO), which is responsible for unclassified information, and the Office of Security and Program Protection (OSPP), which is responsible for classified information.

It is NASA policy to:

a. Protect all NASA information and information systems, both classified and unclassified, in a manner that is commensurate with the national security classification level, sensitivity, value, and criticality of the information.

b. Protect information from unauthorized disclosure, destruction, or modification while the information is being collected, processed, transmitted, stored, or disseminated.

c. Manage all classified and unclassified Information Technology (IT) that is acquired, developed, or used in support of NASA missions, programs, projects, and institutional requirements by use of a process that covers the complete system life cycle.

d. Manage all information systems in a cost-effective manner, guided by the application of sound risk management processes that ensure an appropriate level of integrity, confidentiality, and availability of information in each phase of the system life cycle.

e. Conduct periodic audits of all NASA information systems that process, store, or transmit NASA data.

f. Investigate information security incidents for incident management, forensic investigations, and reports.

g. Ensure basic information security policy requirements, audits, and forensic investigations are implemented across all Centers and activities.

2. APPLICABILITY

a. This directive is applicable to NASA Headquarters and NASA Centers. This directive also applies to NASA Component Facilities and the Jet Propulsion Laboratory (JPL) to the extent specified in their respective contracts. NASA contractors and NASA grantees, to the extent specified in their contract, grant or agreement, and NASA employees shall abide by the requirements of this directive when they perform Agency missions. Facilities, resources, and personnel under a contract or grant from NASA at a college, university, or research establishment are included in the applicability of this directive.

b. For purposes of this directive, the following definitions apply:

(1) "Classified National Security Information (CNSI)" means information that has been determined pursuant to Executive Order (EO) 12958, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(2) "Control" means the exercise of NASA's authority to regulate access to information.

(3) "Information" means any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for or is under the control of NASA.

(4) "Information Security" means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

(5) "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502]

(6) "Information Technology (IT)" means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C. 1401]

(7) "National Security System" means any NASA information system designated as being authorized to process CNSI.

(8) "Unclassified Information" means all information that does not meet the criteria described in EO 12958, as amended. Federal requirements for protecting unclassified information are prescribed in the Federal Information Security Management Act (FISMA) of 2002.

3. AUTHORITY

a. 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended.

b. 5 U.S.C. 552a, the Privacy Act of 1974, as amended.

c. 5 U.S.C. App. III, the Inspector General Act of 1978, as amended.

d. 18 U.S.C. 2510, et seq., the Electronic Communications Privacy Act of 1986, as amended.

e. 18 U.S.C. 2701, the Electronic Communications Privacy Act (ECPA) of 1986, as amended.

f. 40 U.S.C. 1401, Information Technology Management Reform Act of 1996.

g. 44 U.S.C. 3501, et seq., Paperwork Reduction Act of 1995, as amended.

h. 44 U.S.C. 3541 et seq., Federal Information Security Management Act of 2002.

i. Pub. L., 107-347, E-Government Act of 2002.

j. Executive Order 12958, Classified National Security Information, as amended (March 2003).

4. APPLICABLE DOCUMENTS

a. NPR 1600.1, NASA Security Program Procedural Requirements.

b. NPR 2810.1, Security of Information Technology.

c. NPD 9800.1, NASA Office of Inspector General Programs.

d. Federal Information Processing Standards (FIPS). (URL: http://csrc.nist.gov/publications/fips/index.html).

e. National Institute of Standards and Technology (NIST) Special Publications (SPs) 800 Series. (URL: http://csrc.nist.gov/publications/nistpubs/index.html).

5. RESPONSIBILITY

a. The NASA Administrator shall:

(1) Be responsible for:

(a) Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of NASA; and information systems used or operated by NASA or by a contractor of NASA or other organization on behalf of NASA.

(b) Complying with the requirements of FISMA and other Federal laws, related policies, procedures, standards, and guidelines on information security for national security systems issued in accordance with law and as directed by the President.

(c) Ensuring that information security management processes are integrated with NASA's strategic and operational planning processes.

(2) Ensure that senior NASA officials provide information security for the information and information systems that support the operations and assets under their control through:

(a) Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

(b) Determining the levels of information security appropriate to protect such information and information systems for information security classifications and related requirements.

(c) Implementing policies and procedures to cost-effectively reduce risks to an acceptable level.

(d) Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

(3) Delegate to the NASA Chief Information Officer (CIO) the authority to ensure compliance with the requirements imposed on NASA under FISMA sections 3541 et seq.

b. The NASA CIO shall:

(1) Develop and maintain an Agency-wide information security program as required by FISMA. This shall be accomplished by establishing and implementing information security and information system security policies and issuing instructions, memoranda, and bulletins designed to facilitate appropriate protection and accountability of information.

(2) Designate a Senior Agency Information Security Officer (SAISO).

(3) Ensure the development and maintenance of information security policies and procedures to protect unclassified information.

(4) Ensure the development and maintenance of a security certification program compliant with the Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) guidelines Special Publications (SP) 800 series for security authorization of Federal information systems.

(5) For unclassified information systems, shall designate the Agency organization positions for Authorizing Officials (AO), establish AO requirements, and approve the individual AOs who shall have the authority, accountability, and responsibility to formally assume the system risk to Agency operations in accordance with NIST SP 800-37.

(6) Develop and maintain information security procedures and control techniques to address all applicable requirements of NASA's unclassified information security programs.

(7) Train and oversee personnel with responsibilities for information security with respect to such responsibilities.

(8) Issue procedural requirements updates regarding protection and management of unclassified information and IT resources in the form of a NASA Information Technology Requirement (NITR) as necessary to keep pace with the dynamic information security environment.

(9) Charter a NASA Security Operations Center (SOC) to provide consolidated unclassified information security operations and incident response capability that provides Agency-wide visibility and monitoring of NASA networks and systems.

(10) Ensure procedures are established for the referral of suspected and confirmed computer crimes involving unclassified information systems to the NASA Office of Inspector General (OIG) for investigation in a timely manner. Computer crimes include:

(a) Unauthorized access of information.

(b) Compromises of computers.

(c) Compromises of IT resources such as telecommunications systems, command and control systems, and network systems.

(11) Coordinate the initial assessment of suspected computer crimes for unclassified information or information systems, such as unauthorized access of information, compromises of computers, and other IT resources, such as telecommunications systems, command and control systems, and network systems, with the OIG, and other organizations or agencies as appropriate.

(12) Establish a NASA information security capability for unclassified information and information systems with the mission and resources to:

(a) Develop and implement an information security review program designed to ensure that all NASA information systems used to process unclassified information are in compliance with NASA policy, NASA procedural requirements, and Federal guidelines and statutes. Information security reviews shall be coordinated with the NASA OIG Office of Audits to ensure that the review efforts are not duplicated.

(b) Be responsible for the investigation of Sensitive But Unclassified (SBU) information security incidents.

(c) Support counterintelligence reviews, threat assessments, and investigations and issue NASA threat bulletins to protect unclassified information.

(13) Charter a NASA IT Security Advisory Board (ITSAB) to advise the NASA Information Technology Management Board (ITMB), the Deputy CIO for IT Security, and the NASA IT community on information security issues.

c. The NASA Assistant Administrator for Security and Program Protection (SPP) shall:

(1) In collaboration with the NASA CIO, establish a program with multiple security disciplines (e.g., physical, personnel, industrial, communications security (COMSEC), and emanations security (TEMPEST) for the oversight and protection of CNSI to include security control assessments and security authorizations of national security systems in compliance with the national security authorization process.

(2) Establish a NASA COMSEC Material Control System (CMCS).

(3) Appoint a Central Office of Record (COR) which shall:

(a) Set forth minimum National Security Agency standards, procedures, specifications, and guidelines for safeguarding and controlling COMSEC material in NASA's possession.

(b) Investigate and monitor COMSEC incidents.

(4) Coordinate the initial assessment of suspected computer crimes for classified information and information systems with the NASA CIO, the OIG, and other

organizations or agencies as appropriate. Computer crimes include:

(a) Unauthorized access of information.

(b) Compromises of computers.

(c) Compromises of IT resources such as telecommunications systems, command and control systems, and network systems.

(5) In accordance with NPR 1600.1, NASA Security Program Procedural Requirements, establish policy and procedural requirements for appropriate security background investigations of persons who require access to IT systems, applications, and networks operated by or on behalf of NASA.

(6) Conduct counterintelligence reviews and threat assessments and investigations and issue threat bulletins for NASA to protect both classified and unclassified information and information systems.

(7) Provide input to the NASA CIO regarding threat assessments for unclassified information systems.

(8) For classified information security incidents, be responsible for investigation of the information security incidents, cooperate and assist (as requested) by the OIG in its investigation of computer crimes, and refer to the NASA Counterintelligence Director classified security incidents with a counterintelligence nexus.

d. The Associate/Assistant Administrators for Mission Directorates and Mission Support Offices shall:

(1) Participate with the NASA CIO and the Assistant Administrator for SPP in their respective development of NASA information security policies, standards, best practices, and guidance that protects NASA information and IT resources.

(2) Apply these policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software (e.g., IT in spacecraft, aircraft, satellites, facility and system monitoring equipment, and test equipment to include uplink, downlink, and crosslink command and communications) throughout its life cycle and for other embedded IT, through design, development, test, and evaluation, until and through decommissioning.

(3) Ensure that sufficient resources are allocated to address information and information system security requirements developed under this directive for their systems.

(4) Ensure that their respective organizations, including missions, programs, projects, and institutions under their purview, comply with this directive.

(5) Ensure that adequate information security risk management design and planning is conducted to allow for effective cost-benefit analyses of alternate information security postures and of risk acceptance.

(6) The Associate/Assistant Administrators for Mission Directorates and Mission Support Offices may appoint an Information Technology Security Manager (ITSM). The appointed ITSMs shall have the same information security authority, responsibility, and accountability as that of the Center ITSM in accordance with this and other Agency information security directives.

e. The OIG shall be responsible for the investigation of all computer security crimes, such as unauthorized access of information systems, compromises of computers and other IT resources such as telecommunications systems, command and control systems, and network systems. (NPD 9800.1, NASA Office of Inspector General Programs.)

f. The SAISO shall:

(1) Carry out the Agency CIO's responsibilities for information security.

(2) Possess professional qualifications, including training and experience, required to administer the functions described under this section.

(3) Be responsible for information security duties.

(4) Establish an office with the mission and resources for information security operations, security governance, security architecture and engineering, and cyber-threat analysis to assist in ensuring Agency compliance with FISMA section 3541 et seq.

(5) Provide management and oversight of the NASA SOC.

(6) Manage the Agency's information security program and activities for unclassified information and information systems, including the preparation and maintenance of NPR 2810.1, Security of Information Technology.

(7) Provide program management of the Agency's unclassified information security programs and projects.

(8) Serve as the NASA Information System Risk Executive responsible to ensure that security risk-related considerations and risk management of individual information systems are consistent across the Agency, are viewed from an Agency-wide and strategic goal perspective, and reflect the Agency's information system risk tolerance affecting mission/business success.

(9) Establish and manage the Agency information security performance metrics program.

g. The Center Directors and the Director for Headquarters Operations shall:

(1) Ensure compliance with this directive, NASA policies, procedures, requirements, and the Federal information security policy for activities under their purview.

(2) Designate a Center ITSM who shall:

(a) Assist the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws, directives, policies, standards, and guidelines.

(b) Be the Senior Center Information Security Officer for interaction with the SAISO.

(c) Head an office with the mission and resources for information security operations, security governance, and security architecture and engineering to assist the Center CIO in the compliance with FISMA section 3541 et seq.

(d) Participate as the Center's voting member of the Agency ITSAB.

(3) Ensure the Center CIO has adequate staff, resources, budget, and authority to

implement the information security programs within the purview of the Center.

(4) Make available qualified personnel to support periodic security assessments conducted by the Agency OCIO.

h. Center CIOs and the Headquarters Operations CIO, for information and information systems under their purview, shall:

(1) Be responsible and accountable for the protection of the information and the IT resources under their cognizance.

(2) Be responsible and accountable for compliance with this directive, NASA information security policies and procedures and the Federal information security laws, directives, policies, standards, and guidelines.

(3) For unclassified security incidents, be responsible for the coordination of investigations of information security incidents and the investigation coordination with the NASA CIO to include:

(a) Referral of an information security incident to an investigating authority shall be made in consultation with the SAISO and affected ITSMs.

(b) The Center CIO and ITSM shall cooperate and assist, as requested, by the NASA OIG in its investigation of computer crimes.

(c) Information security incidents with a counterintelligence nexus shall be referred to the NASA Counterintelligence Director.

6. DELEGATION OF AUTHORITY

The NASA CIO is authorized to ensure compliance with the requirements imposed on the Agency under FISMA, subchapter 3544.

7. MEASUREMENTS

The effectiveness of this directive will be assessed as follows:

a. Measurements shall be collected and evaluated by the NASA CIO to assess the effectiveness of this policy directive at least annually by measuring the degree of compliance with assignments of responsibility for information security, establishment of security plans, review of security controls, and documented authorizations that security plans are adequately implemented.

b. Measurements shall be collected and evaluated by the NASA CIO at least annually to assess trends involving information security incidents and trends for tracking metrics involving the cost, schedule impact, and effect on mission, program, and project performance attributed to the loss, alteration, unavailability, misuse, or unauthorized access to or modification of Agency information or IT resources.

8. CANCELLATION

NPD 2810.1C, NASA Information Security Policy, dated April 07, 2004.

/s/ Christopher J. Scolese
Acting Administrator

ATTACHMENT A: (TEXT)

None.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS